10106514847

2

日 本 国 特 許 庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日
Date of Application: ２００２年 ９月２０日

出 願 番 号
Application Number: 特願２００２－２７５９７３

[ST. 10/C]: ［ＪＰ２００２－２７５９７３］

出 願 人
Applicant(s): 株式会社リコー

２００３年 ８月２５日

特許庁長官
Commissioner,
Japan Patent Office 今井康夫

出証番号 出証特２００３－３０６９４８７

【書類名】　特許願
【整理番号】　0201598
【提出日】　平成14年 9月20日
【あて先】　特許庁長官　太田　信一郎　殿
【国際特許分類】　G06F 17/60
【発明の名称】　セキュリティポリシーに基づいた文書の読み取り装置、読み取り方法、ネットワーク配信を行う装置及びネットワーク配信を行う方法
【請求項の数】　32
【発明者】
【住所又は居所】　東京都大田区中馬込１丁目３番６号　株式会社リコー内
【氏名】　斉藤　敦久
【発明者】
【住所又は居所】　東京都大田区中馬込１丁目３番６号　株式会社リコー内
【氏名】　金井　洋一
【発明者】
【住所又は居所】　東京都大田区中馬込１丁目３番６号　株式会社リコー内
【氏名】　谷内田　益義
【特許出願人】
【識別番号】　000006747
【氏名又は名称】　株式会社リコー
【代理人】
【識別番号】　100070150
【弁理士】
【氏名又は名称】　伊東　忠彦
【手数料の表示】
【予納台帳番号】　002989
【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　セキュリティポリシーに基づいた文書の読み取り装置、読み取り方法、ネットワーク配信を行う装置及びネットワーク配信を行う方法

【特許請求の範囲】

【請求項１】　少なくともユーザカテゴリーとセキュリティレベルを有するユーザ属性と、

少なくとも文書カテゴリーとセキュリティレベルを有する文書属性と、

読み取りを許可する前記文書属性と前記ユーザ属性との組み合わせと、

前記組み合わせで読み取りを実行する場合の要件と、

を備えるセキュリティポリシーに基づいた文書の読み取り方法であって、

前記読み取り方法は、

前記ユーザ属性を取得するステップと、

読み取りを行った前記文書のデータから、前記文書の前記文書属性を取得するステップと、

取得した前記ユーザ属性と前記文書属性との組み合わせに対して、読み取りが許可されているか否かを、前記セキュリティポリシーに基づいて判断するステップと、

前記読み取りが許可されていないと判断した場合には、前記読み取りを行った前記データを破棄して終了するステップと、

前記読み取りが許可されていると判断した場合には、対応する要件を前記セキュリティポリシーから抽出するステップと、

抽出されるべき前記要件が、前記セキュリティポリシー内に存在しない場合には、前記文書の読み取りを行って終了するステップと、

抽出されるべき前記要件が、前記セキュリティポリシー内に存在する場合には、すべての前記要件を、前記読み取る方法で実行可能であるかを判定するステップと、

実行可能でない前記要件が、存在する場合には、前記文書の読み取りを行ったデータを破棄して終了するステップと、

すべての要件を実行可能である場合には、抽出された前記要件を満たして、前

記文書の読み取りを行って終了するステップと、
を有する、セキュリティポリシーに基づいた文書の読み取り方法。

【請求項２】　前記実行可能な要件は、前記読み取った文書データに電子透かしを埋め込むことである、請求項１に記載のセキュリティポリシーに基づいた文書の読み取り方法。

【請求項３】　前記実行可能な要件は、前記読み取った文書データに表示可能なラベルを埋め込むことである、請求項１あるいは２に記載のセキュリティポリシーに基づいた文書の読み取り方法。

【請求項４】　前記表示可能なラベルは、少なくとも読み取りを指示したユーザの認証データと、読み取りを指示した時点のタイムスタンプを含む、請求項３に記載のセキュリティポリシーに基づいた文書の読み取り方法。

【請求項５】　前記実行可能な要件は、少なくとも読み取りを指示したユーザの認証データと、読み取り対象の文書データと、読み取りを指示した時点のタイムスタンプをログに記録を行うことである、請求項１乃至４のうち何れか一項に記載のセキュリティポリシーに基づいた文書の読み取り方法。

【請求項６】　請求項１乃至５のうち何れか一項に記載のセキュリティポリシーに基づいた文書の読み取り方法を、コンピュータに実行させる、セキュリティポリシーに基づいた文書の読み取りプログラム。

【請求項７】　請求項６に記載のプログラムを記憶したコンピュータ読み取り可能な記憶媒体。

【請求項８】　請求項６に記載のプログラムを、コンピュータにネットワークを介して配信するプログラム伝送装置。

【請求項９】　少なくともユーザカテゴリーとセキュリティレベルを有するユーザ属性と、
　少なくとも文書カテゴリーとセキュリティレベルを有する文書属性と、
　読み取りを許可する前記文書属性と前記ユーザ属性との組み合わせと、
　前記組み合わせで読み取りを実行する場合の要件と、
を備えるセキュリティポリシーに基づいた文書の読み取り装置であって、
　前記読み取り装置は、

前記ユーザ属性を取得する手段と、

読み取りを行った前記文書のデータから、前記文書の前記文書属性を取得する手段と、

取得した前記ユーザ属性と前記文書属性との組み合わせに対して、読み取りが許可されているか否かを、前記セキュリティポリシーに基づいて判断する手段と、

前記読み取りが許可されていないと判断した場合には、前記読み取りを行ったデータを破棄して終了する手段と、

前記読み取りが許可されていると判断した場合には、対応する要件を前記セキュリティポリシーから抽出する手段と、

抽出されるべき前記要件が、前記セキュリティポリシー内に存在しない場合には、前記文書の読み取りを行って終了する手段と、

抽出されるべき前記要件が、前記セキュリティポリシー内に存在する場合には、すべての前記要件を、前記読み取り方法で実行可能であるかを判定する手段と、

実行可能でない前記要件が、存在する場合には、前記文書の読み取りを行ったデータを破棄して終了する手段と、

すべての要件を実行可能である場合には、抽出された前記要件を満たして、前記文書の読み取りを行って終了する手段と、

を有する、セキュリティポリシーに基づいた文書の読み取り装置。

【請求項１０】　前記実行可能な要件は、前記読み取った文書データに電子透かしを埋め込むことである、請求項９に記載のセキュリティポリシーに基づいた文書の読み取り装置。

【請求項１１】　前記実行可能な要件は、前記読み取った文書データに表示可能なラベルを埋め込むことである、請求項９あるいは１０に記載のセキュリティポリシーに基づいた文書の読み取り装置。

【請求項１２】　前記表示可能なラベルは、少なくとも読み取りを指示したユーザの認証データと、読み取りを指示した時点のタイムスタンプを含む、請求項１１に記載のセキュリティポリシーに基づいた文書の読み取り装置。

【請求項１３】　前記実行可能な要件は、少なくとも読み取りを指示したユーザの認証データと、読み取り対象の文書データと、読み取りを指示した時点のタイムスタンプをログに記録を行うことである、請求項９乃至１２のうち何れか一項に記載のセキュリティポリシーに基づいた文書の読み取り装置。

【請求項１４】　少なくともユーザカテゴリーとセキュリティレベルを有するユーザ属性と、

少なくとも文書カテゴリーとセキュリティレベルを有する文書属性と、

読み取りを許可する前記文書属性と前記ユーザ属性との組み合わせと、

前記組み合わせで読み取りを実行する場合の要件と、

ネットワーク配信を許可する前記文書属性と前記ユーザ属性との組み合わせと、

前記組み合わせでネットワーク配信を実行する場合の要件と、

を備えるセキュリティポリシーに基づいて文書を読み取り且つネットワーク配信を行う方法であって、

前記文書を読み取り且つネットワーク配信を行う方法は、

前記ユーザ属性を取得するステップと、

読み取りを行った前記文書のデータから、前記文書の前記文書属性を取得するステップと、

取得した前記ユーザ属性と前記文書属性との組み合わせに対して、前記文書の読み取りとネットワーク配信が許可されているか否かを、前記セキュリティポリシーに基づいて判断するステップと、

前記読み取りとネットワーク配信が許可されていないと判断した場合には、前記読み取りを行った前記データを破棄して終了するステップと、

前記文書の読み取りとネットワーク配信が許可されていると判断した場合には、対応する要件を前記セキュリティポリシーから抽出するステップと、

抽出されるべき前記要件が、前記セキュリティポリシー内に存在しない場合には、前記文書の読み取りとネットワーク配信を行って終了するステップと、

抽出されるべき前記要件が、前記セキュリティポリシー内に存在する場合には、すべての前記要件が前記文書の読み取りとネットワーク配信を行う方法で実行

可能であるかを判定するステップと、

実行可能でない前記要件が、存在する場合には、前記文書の読み取りを行ったデータを破棄して終了するステップと、

すべての要件を実行可能である場合には、抽出された前記要件を満たして、前記文書の読み取りとネットワーク配信を行って終了するステップと、

を有するセキュリティポリシーに基づいて文書を読み取り且つネットワーク配信を行う方法。

【請求項１５】　前記実行可能な要件が、前記読み取った文書データに電子透かしを埋め込むことである、請求項１４に記載のセキュリティポリシーに基づいて文書を読み取り且つネットワーク配信を行う方法。

【請求項１６】　前記実行対応可能な要件は、前記読み取った文書データに表示可能なラベルを埋め込むことである、請求項１４あるいは１５に記載のセキュリティポリシーに基づいて文書を読み取り且つネットワーク配信を行う方法。

【請求項１７】　前記表示可能なラベルは、少なくとも読み取りとネットワーク配信を指示したユーザの認証データと、読み取りを指示した時点のタイムスタンプを含む、請求項１５に記載のセキュリティポリシーに基づいて文書を読み取り且つネットワーク配信を行う方法。

【請求項１８】　前記実行可能な要件は、少なくとも読み取りとネットワーク配信を指示したユーザの認証データと、ネットワーク配信先の情報と、読み取り対象の文書データと、読み取りを指示した時点のタイムスタンプをログに記録を行うことである、請求項１４乃至１７のうち何れか一項に記載のセキュリティポリシーに基づいて文書を読み取り且つネットワーク配信を行う方法。

【請求項１９】　前記実行可能な要件は、文書データを印刷不可能なデータに変換してネットワーク配信を行うことである、請求項１４乃至１８のうち何れか一項に記載のセキュリティポリシーに基づいて文書を読み取り且つネットワーク配信を行う方法。

【請求項２０】　前記印刷不可能なデータは、印刷禁止属性を持ったＰＤＦファイルである、請求項１９に記載のセキュリティポリシーに基づいて文書を読み取り且つネットワーク配信を行う方法。

【請求項２１】　前記実行可能な要件が、信頼できるチャネルを利用してネットワーク配信を行うことである、請求項１４乃至２０のうち何れか一項に記載のセキュリティポリシーに基づいて文書を読み取り且つネットワーク配信を行う方法。

【請求項２２】　請求項１４乃至２１のうち何れか一項に記載のセキュリティポリシーに基づいて文書を読み取り且つネットワーク配信を行う方法をコンピュータに実行させる、セキュリティポリシーに基づいて文書を読み取り且つネットワーク配信を行うプログラム。

【請求項２３】　請求項２２に記載のプログラムを記憶したコンピュータ読み取り可能な記憶媒体。

【請求項２４】　請求項２２に記載のプログラムをコンピュータにネットワーク配信するプログラム伝送装置。

【請求項２５】　少なくともユーザカテゴリーとセキュリティレベルを有するユーザ属性と、

少なくとも文書カテゴリーとセキュリティレベルを有する文書属性と、

読み取りを許可する前記文書属性と前記ユーザ属性との組み合わせと、

前記組み合わせで読み取りを実行する場合の要件と、

ネットワーク配信を許可する前記文書属性と前記ユーザ属性との組み合わせと、

前記組み合わせでネットワーク配信を実行する場合の要件と、

を備えるセキュリティポリシーに基づいて文書を読み取り且つネットワーク配信を行う装置であって、

前記文書を読み取り且つネットワーク配信を行う装置は、

前記ユーザ属性を取得する手段と、

読み取りを行った前記文書のデータから、前記文書の前記文書属性を取得する手段と、

取得した前記ユーザ属性と前記文書属性との組み合わせに対して、読み取りとネットワーク配信が許可されているか否かを、前記セキュリティポリシーに基づいて判断する手段と、

前記文書を読み取り且つネットワーク配信を行うことが許可されていないと判断した場合には、前記読み取りを行ったデータを破棄して終了する手段と、

前記文書を読み取り且つネットワーク配信を行うことが許可されていると判断した場合には、対応する要件を前記セキュリティポリシーから抽出する手段と、

抽出されるべき前記要件が、前記セキュリティポリシー内に存在しない場合には、前記文書の読み取りとネットワーク配信を行って終了する手段と、

抽出されるべき前記要件が、前記セキュリティポリシー内に存在する場合には、すべての前記要件が前記文書を読み取り且つネットワーク配信を行う方法で実行可能であるかを判定する手段と、

実行可能でない前記要件が、存在する場合には、前記文書の読み取りを行ったデータを破棄して終了する手段と、

すべての前記要件が実行可能である場合には、抽出された前記要件を満たして、前記文書を読み取り且つネットワーク配信を行って終了する手段と、

を有する、セキュリティポリシーに基づいて文書を読み取り且つネットワーク配信を行う装置。

【請求項２６】　前記実行可能な要件は、前記読み取った文書データに電子透かしを埋め込むことである、請求項２５に記載のセキュリティポリシーに基づいて文書を読み取り且つネットワーク配信を行う装置。

【請求項２７】　前記実行可能な要件が、前記読み取った文書データに表示可能なラベルを埋め込むことである、請求項２５あるいは２６に記載のセキュリティポリシーに基づいた文書の読み取りとネットワーク配信を行う装置。

【請求項２８】　前記表示可能なラベルは、少なくとも読み取りとネットワーク配信を指示したユーザの認証データと、読み取りを指示した時点のタイムスタンプを含む、請求項２７に記載のセキュリティポリシーに基づいて文書を読み取り且つネットワーク配信を行う装置。

【請求項２９】　前記実行可能な要件は、少なくとも読み取りとネットワーク配信を指示したユーザの認証データと、ネットワーク配信先の情報と、読み取り対象の文書データと、読み取りを指示した時点のタイムスタンプをログに記録を行うことである、請求項２５乃至２８のうち何れか一項に記載のセキュリティポ

リシーに基づいて文書を読み取り且つネットワーク配信を行う装置。

【請求項３０】　前記実行可能な要件が、文書データを印刷不可能なデータに変換してネットワーク配信を行うことである、請求項２５乃至２９のうち何れか一項に記載のセキュリティポリシーに基づいて文書を読み取り且つネットワーク配信を行う装置。

【請求項３１】　前記印刷不可能なデータは、印刷禁止属性を持ったＰＤＦファイルである、請求項３０に記載のセキュリティポリシーに基づいて文書を読み取り且つネットワーク配信を行う装置。

【請求項３２】　前記実行可能な要件が、信頼できるチャネルを利用してネットワーク配信を行うことである、請求項２５乃至３１のうち何れか一項に記載のセキュリティポリシーに基づいて文書を読み取り且つネットワーク配信を行う装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、情報システムのセキュリティを確保するシステムに関し、特に、セキュリティポリシーに基づいた文書の読み取りとネットワーク配信を行う方法、装置、プログラム、記憶媒体、及び伝送装置に関連する。

【０００２】

【従来の技術】

オフィスに代表されるような文書を扱うフィールドでは、その文書のセキュリティをコントロールしたいという要望が、常に存在する。例えば秘密の文書を複写する際には管理責任者の許可を得なければならない等，特に情報のコンテナであるドキュメントに対するポリシー，中でも機密保持に関するポリシーの制御が重要視される。一般に、情報システムのセキュリティ確保は機密性、完全性、可用性の確保に大別されるが、完全性や可用性はシステムの管理者が適切に運営、管理すれば実質上問題のないレベルまで確保できることが多い。これに対して、機密性の確保のためには、ユーザ組織に所属するメンバに、ポリシーを共有及び徹底させなければならないためであろうと推測される。

【０００３】

現実に多くの企業では文書管理規定などを設け、セキュリティをコントロールしようとしている。しかし、実際のオフィスシステムにおけるセキュリティの確保については、文書についてのセキュリティではなく、オフィスシステムを構成するさまざまな機器に関して、個別にセキュリティ設定を行う必要がある。

【０００４】

セキュリティポリシーに基づいてアクセス制御を行う方法に関する従来技術としては、種々のものが挙げられる（特許文献１から、特許文献６）。

【０００５】

例えば、アクセス制御において、条件付のアクセス許可を評価することが記載されている（特許文献１）。

【０００６】

また、例えば、情報セキュリティポリシーに従った企業情報システムのセキュリティ管理、監査の簡単化について記載されている(特許文献２)。

【０００７】

しかし、特に、上述の特許文献１では、データファイルへのアクセス制御システムで、アクセス後のデータの処理、特に読み取りなどには言及されていない。

【０００８】

また、上述の特許文献２では、セキュリティーポリシー、システム、制御手段から構成され、それぞれの組み合わせを登録してあるＤＢ（データベース）から制御手段を抽出して、システムをポリシーに合うように制御する手段を有しているがしかし、その状態を監査する手段では、システムに対して登録された制御手段で制御するだけであり、実現の自由度が低い。

【０００９】

【特許文献１】

特開２００１－１８４２６４号公報

【特許文献２】

特開２００１－２７３３８８号公報

【特許文献３】

特開２００１－３３７８６４号公報

【特許文献４】

特開平０９－２９３０３６号公報

【特許文献５】

特開平０７－１４１２９６号公報

【特許文献６】

特許第０２７３５９６６号公報。

【００１０】

【発明が解決しようとする課題】

このようなセキュリティの設定方法では、文書印刷のセキュリティ設定をする場合には、第１に、設定者が、さまざまな機器のセキュリティに関する知識を必要とする。そして、第２には、すべての機器に対してセキュリティが、一つ一つ設定される必要がある。第３には、システムの全体がどのようなセキュリティ状態になっているのかを容易に把握することが必要であるが、把握しにくい。そして、第４に、個々の機器にセキュリティ設定がされていても、実際に文書のセキュリティが守られていることが実感できない。このように、実際のオフィスシステムにおけるセキュリティの確保については、以上のようなの問題点がある。本発明は、上述の問題点を解決することを目的とする。

【００１１】

特に本発明の目的は、文書に関するセキュリティポリシーに基づいて、紙文書の読み取り、ネットワークへの配信を行う方法、その方法を実行するプログラム、そのプログラムを記憶した記憶媒体、文書の伝送装置および文書の印刷装置を提供することである。

【００１２】

【課題を解決するための手段】

上記目的は、以下の本発明により解決される。

【００１３】

請求項１に記載の発明では、セキュリティポリシーに基づいた文書の読み取り方法は、少なくともユーザカテゴリーとセキュリティレベルを有するユーザ属性

と、

少なくとも文書カテゴリーとセキュリティレベルを有する文書属性と、

読み取りを許可する前記文書属性と前記ユーザ属性との組み合わせと、

前記組み合わせで読み取りを実行する場合の要件と、

を備えるセキュリティポリシーに基づいた文書の読み取り方法であって、

前記読み取り方法は、

前記ユーザ属性を取得するステップと、

読み取りを行った前記文書のデータから、前記文書の前記文書属性を取得するステップと、

取得した前記ユーザ属性と前記文書属性との組み合わせに対して、読み取りが許可されているか否かを、前記セキュリティポリシーに基づいて判断するステップと、

前記読み取りが許可されていないと判断した場合には、前記読み取りを行った前記データを破棄して終了するステップと、

前記読み取りが許可されていると判断した場合には、対応する要件を前記セキュリティポリシーから抽出するステップと、

抽出されるべき前記要件が、前記セキュリティポリシー内に存在しない場合には、前記文書の読み取りを行って終了するステップと、

抽出されるべき前記要件が、前記セキュリティポリシー内に存在する場合には、すべての前記要件を、前記読み取る方法で実行可能であるかを判定するステップと、

実行可能でない前記要件が、存在する場合には、前記文書の読み取りを行ったデータを破棄して終了するステップと、

すべての要件を実行可能である場合には、抽出された前記要件を満たして、前記文書の読み取りを行って終了するステップと、

を有する。

【００１４】

請求項２に記載の発明では、前記実行可能な要件は、前記読み取った文書データに電子透かしを埋め込むことである。

【００１５】

請求項３に記載の発明では、前記実行可能な要件は、前記読み取った文書データに表示可能なラベルを埋め込むことである。

【００１６】

請求項４に記載の発明では、前記表示可能なラベルは、少なくとも読み取りを指示したユーザの認証データと、読み取りを指示した時点のタイムスタンプを含む。

【００１７】

請求項５に記載の発明では、前記実行可能な要件は、少なくとも読み取りを指示したユーザの認証データと、読み取り対象の文書データと、読み取りを指示した時点のタイムスタンプをログに記録を行うことである。

【００１８】

請求項６に記載の発明は、セキュリティポリシーに基づいた文書の読み取り方法を、コンピュータに実行させる、セキュリティポリシーに基づいた文書の読み取りプログラム。

【００１９】

請求項７に記載の発明は、そのプログラムを記憶したコンピュータ読み取り可能な記憶媒体である。

【００２０】

請求項８に記載の発明は、そのプログラムを、コンピュータにネットワークを介して配信するプログラム伝送装置である。

【００２１】

請求項９に記載の発明では、セキュリティポリシーに基づいた文書の読み取り装置は、少なくともユーザカテゴリーとセキュリティレベルを有するユーザ属性と、

少なくとも文書カテゴリーとセキュリティレベルを有する文書属性と、

読み取りを許可する前記文書属性と前記ユーザ属性との組み合わせと、

前記組み合わせで読み取りを実行する場合の要件と、

を備えるセキュリティポリシーに基づいた文書の読み取り装置であって、

前記読み取り装置は、

前記ユーザ属性を取得する手段と、

読み取りを行った前記文書のデータから、前記文書の前記文書属性を取得する手段と、

取得した前記ユーザ属性と前記文書属性との組み合わせに対して、読み取りが許可されているか否かを、前記セキュリティポリシーに基づいて判断する手段と、

前記読み取りが許可されていないと判断した場合には、前記読み取りを行ったデータを破棄して終了する手段と、

前記読み取りが許可されていると判断した場合には、対応する要件を前記セキュリティポリシーから抽出する手段と、

抽出されるべき前記要件が、前記セキュリティポリシー内に存在しない場合には、前記文書の読み取りを行って終了する手段と、

抽出されるべき前記要件が、前記セキュリティポリシー内に存在する場合には、すべての前記要件を、前記読み取り方法で実行可能であるかを判定する手段と、

実行可能でない前記要件が、存在する場合には、前記文書の読み取りを行ったデータを破棄して終了する手段と、

すべての要件を実行可能である場合には、抽出された前記要件を満たして、前記文書の読み取りを行って終了する手段と、

を有する。

【００２２】

請求項１０に記載の発明では、前記実行可能な要件は、前記読み取った文書データに電子透かしを埋め込むことである。

【００２３】

請求項１１に記載の発明では、前記実行可能な要件は、前記読み取った文書データに表示可能なラベルを埋め込むことである。

【００２４】

請求項１２に記載の発明では、前記表示可能なラベルは、少なくとも読み取り

を指示したユーザの認証データと、読み取りを指示した時点のタイムスタンプを含む。

【００２５】

請求項１３に記載の発明では、前記実行可能な要件は、少なくとも読み取りを指示したユーザの認証データと、読み取り対象の文書データと、読み取りを指示した時点のタイムスタンプをログに記録を行うことである。

【００２６】

請求項１４に記載の発明では、セキュリティポリシーに基づいて文書を読み取り且つネットワーク配信を行う方法は、少なくともユーザカテゴリーとセキュリティレベルを有するユーザ属性と、

少なくとも文書カテゴリーとセキュリティレベルを有する文書属性と、

読み取りを許可する前記文書属性と前記ユーザ属性との組み合わせと、

前記組み合わせで読み取りを実行する場合の要件と、

ネットワーク配信を許可する前記文書属性と前記ユーザ属性との組み合わせと、

前記組み合わせでネットワーク配信を実行する場合の要件と、

を備えるセキュリティポリシーに基づいて文書を読み取り且つネットワーク配信を行う方法であって、

前記文書を読み取り且つネットワーク配信を行う方法は、

前記ユーザ属性を取得するステップと、

読み取りを行った前記文書のデータから、前記文書の前記文書属性を取得するステップと、

取得した前記ユーザ属性と前記文書属性との組み合わせに対して、前記文書の読み取りとネットワーク配信が許可されているか否かを、前記セキュリティポリシーに基づいて判断するステップと、

前記読み取りとネットワーク配信が許可されていないと判断した場合には、前記読み取りを行った前記データを破棄して終了するステップと、

前記文書の読み取りとネットワーク配信が許可されていると判断した場合には、対応する要件を前記セキュリティポリシーから抽出するステップと、

抽出されるべき前記要件が、前記セキュリティポリシー内に存在しない場合には、前記文書の読み取りとネットワーク配信を行って終了するステップと、

抽出されるべき前記要件が、前記セキュリティポリシー内に存在する場合には、すべての前記要件が前記文書の読み取りとネットワーク配信を行う方法で実行可能であるかを判定するステップと、

実行可能でない前記要件が、存在する場合には、前記文書の読み取りを行ったデータを破棄して終了するステップと、

すべての要件を実行可能である場合には、抽出された前記要件を満たして、前記文書の読み取りとネットワーク配信を行って終了するステップと、

を有する。

【００２７】

請求項１５に記載の発明では、前記実行可能な要件が、前記読み取った文書データに電子透かしを埋め込むことである。

【００２８】

請求項１６に記載の発明では、前記実行対応可能な要件は、前記読み取った文書データに表示可能なラベルを埋め込むことである。

【００２９】

請求項１７に記載の発明では、前記表示可能なラベルは、少なくとも読み取りとネットワーク配信を指示したユーザの認証データと、読み取りを指示した時点のタイムスタンプを含む。

【００３０】

請求項１８に記載の発明では、前記実行可能な要件は、少なくとも読み取りとネットワーク配信を指示したユーザの認証データと、ネットワーク配信先の情報と、読み取り対象の文書データと、読み取りを指示した時点のタイムスタンプをログに記録を行うことである。

【００３１】

請求項１９に記載の発明では、前記実行可能な要件は、文書データを印刷不可能なデータに変換してネットワーク配信を行うことである。

【００３２】

請求項２０に記載の発明では、前記印刷不可能なデータは、印刷禁止属性を持ったＰＤＦファイルである。

【００３３】

請求項２１に記載の発明では、前記実行可能な要件が、信頼できるチャネルを利用してネットワーク配信を行うことである。

【００３４】

請求項２２に記載の発明は、セキュリティポリシーに基づいて文書を読み取り且つネットワーク配信を行う方法をコンピュータに実行させる、セキュリティポリシーに基づいて文書を読み取り且つネットワーク配信を行うプログラムである。

【００３５】

請求項２３に記載の発明は、そのプログラムを記憶したコンピュータ読み取り可能な記憶媒体である。

【００３６】

請求項２４に記載の発明は、そのプログラムをコンピュータにネットワーク配信するプログラム伝送装置である。

【００３７】

請求項２５に記載の発明では、セキュリティポリシーに基づいて文書を読み取り且つネットワーク配信を行う装置は、少なくともユーザカテゴリーとセキュリティレベルを有するユーザ属性と、

少なくとも文書カテゴリーとセキュリティレベルを有する文書属性と、

読み取りを許可する前記文書属性と前記ユーザ属性との組み合わせと、

前記組み合わせで読み取りを実行する場合の要件と、

ネットワーク配信を許可する前記文書属性と前記ユーザ属性との組み合わせと、

前記組み合わせでネットワーク配信を実行する場合の要件と、

を備えるセキュリティポリシーに基づいて文書を読み取り且つネットワーク配信を行う装置であって、

前記文書を読み取り且つネットワーク配信を行う装置は、

前記ユーザ属性を取得する手段と、

読み取りを行った前記文書のデータから、前記文書の前記文書属性を取得する手段と、

取得した前記ユーザ属性と前記文書属性との組み合わせに対して、読み取りとネットワーク配信が許可されているか否かを、前記セキュリティポリシーに基づいて判断する手段と、

前記文書を読み取り且つネットワーク配信を行うことが許可されていないと判断した場合には、前記読み取りを行ったデータを破棄して終了する手段と、

前記文書を読み取り且つネットワーク配信を行うことが許可されていると判断した場合には、対応する要件を前記セキュリティポリシーから抽出する手段と、

抽出されるべき前記要件が、前記セキュリティポリシー内に存在しない場合には、前記文書の読み取りとネットワーク配信を行って終了する手段と、

抽出されるべき前記要件が、前記セキュリティポリシー内に存在する場合には、すべての前記要件が前記文書を読み取り且つネットワーク配信を行う方法で実行可能であるかを判定する手段と、

実行可能でない前記要件が、存在する場合には、前記文書の読み取りを行ったデータを破棄して終了する手段と、

すべての前記要件が実行可能である場合には、抽出された前記要件を満たして、前記文書を読み取り且つネットワーク配信を行って終了する手段と、

を有する。

【００３８】

請求項２６に記載の発明では、前記実行可能な要件は、前記読み取った文書データに電子透かしを埋め込むことである。

【００３９】

請求項２７に記載の発明では、前記実行可能な要件が、前記読み取った文書データに表示可能なラベルを埋め込むことである。

【００４０】

請求項２８に記載の発明では、前記表示可能なラベルは、少なくとも読み取りとネットワーク配信を指示したユーザの認証データと、読み取りを指示した時点

のタイムスタンプを含む。

【００４１】

請求項２９に記載の発明では、前記実行可能な要件は、少なくとも読み取りとネットワーク配信を指示したユーザの認証データと、ネットワーク配信先の情報と、読み取り対象の文書データと、読み取りを指示した時点のタイムスタンプをログに記録を行うことである。

【００４２】

請求項３０に記載の発明では、前記実行可能な要件が、文書データを印刷不可能なデータに変換してネットワーク配信を行うことである。

【００４３】

請求項３１に記載の発明では、前記印刷不可能なデータは、印刷禁止属性を持ったＰＤＦファイルである。

【００４４】

請求項３２に記載の発明では、前記実行可能な要件が、信頼できるチャネルを利用してネットワーク配信を行うことである。

【００４５】

以上本発明により、文書に関するセキュリティポリシーに基づいて、紙文書の読み取り、ネットワークへの配信を行う方法、その方法を実行するプログラム、そのプログラムを記憶した記憶媒体、文書の伝送装置および文書の印刷装置を提供することができる。

【００４６】

【発明の実施の形態】

本発明の実施例を、図１及び図２を参照して以下に詳細に説明する。

【００４７】

図１は、本発明の実施例の文書読み取り装置の構成を示す図である。また、図２は、ＸＭＬ（Ｅｘｔｅｎｓｉｂｌｅ　Ｍａｒｋｕｐ　Ｌａｎｇｕａｇｅ）により記述した、本発明の実施例のセキュリティポリシーを示す。

【００４８】

図１に示す本発明の実施例の文書読み取り装置１００は、主に、オペレーショ

ンパネル１０１、データベース１０２、ユーザ属性取得手段１０３、文書属性取得手段１０４、セキュリティーポリシー１０５、読み取り手段１０６、読み取りデータ１０７及びネットワークポート１０８より構成される。

【００４９】

オペレーションパネル１０１には、読み取り支持１１０が入力される。

【００５０】

図１においては、読み取り装置は、専用のハードウェアにより構成するように記載されているが、汎用のコンピュータとそのコンピュータ上で実行されるプログラムにより構成されても良い。また、以下に説明する本発明の実施例をコンピュータ上で実行するプログラムは、コンピュータにより読み出し可能な記録媒体に記録され、その実行前に、コンピュータにより読みこまれる。また、このようなプログラムは、コンピュータネットワークを介して配信されることも可能である。

【００５１】

図２は、ＸＭＬにより記述した、セキュリティポリシーであり、つぎのようにルール１からルール３を示す。

【００５２】

ルール１は、図２の第４行目の<acc_rule>から、第１０行目の<user_security_level>ANY</user_security_level>までの部分及び、第１１行目<operation>から、第１４行目</operation>までの部分により記述される。

【００５３】

第５行目の <doc_category>ANY</doc_category>は、文書カテゴリーにかかわりなくルール１が適用されることを示す。

【００５４】

第６行目の<doc_security_level>basic</doc_security_level>は、文書のセキュリティレベルがbasicのときを示す。

【００５５】

第９行目の<user_category>ANY</user_category>は、ユーザのカテゴリーにかかわりないこととを示す。

【００５６】

第１０行目の<user_security_level>ANY</user_security_level>は、ユーザのセキュリティレベルにかかわりないことを示す。

【００５７】

更に第１２行目と第１３行目の<name>scan</name>及び<allowed/>は、読み取りは要件なく許可されることを示す。

【００５８】

従って、ルール１では、第５行目、第６行目、第９行目、第１０行目、第１２行目及び第１３行目により、文書カテゴリーにかかわりなく、文書のセキュリティレベルが”basic”の場合には、ユーザのカテゴリーにかかわりなく、且つ、ユーザのセキュリティレベルにかかわりなく、読み取りは要件なく許可される。

【００５９】

次に、ルール２は、図２の第４行目の<acc_rule>から、第１０行目の<user_security_level>ANY</user_security_level>までの部分及び、第１５行目<operation>から、第２０行目</operation>までの部分により記述される。

【００６０】

第５行目の <doc_category>ANY</doc_category>は、文書カテゴリーにかかわりなくルール２が適用されることを示している。

【００６１】

第６行目の<doc_security_level>basic</doc_security_level>は、文書のセキュリティレベルがbasicのときを示す。

【００６２】

第９行目の<user_category>ANY</user_category>は、ユーザのカテゴリーにかかわりないことを示す。

【００６３】

第１０行目の<user_security_level>ANY</user_security_level>は、ユーザのセキュリティレベルにかかわりないことを示す。

【００６４】

更に、第１６行目から第１９行目の

<name>net_delivery</name>

<requirement>audit</requirement>

<requirement>print_restriction</requirement>

<requirement>trusted_channel</requirement>

は、ネットワーク配信は、「ログを記録すること」と、「プリント制限をかけること」、「信頼できるチャネルを使用すること」の要件を満たすときに許可されることを示す。

【００６５】

従って、ルール２では、第５行目、第６行目、第９行目、第１０行目、第１６行目から第１９行目により、文書カテゴリーにかかわりなく、文書のセキュリティレベルが”basic”の場合には、ユーザのカテゴリーにかかわりなく、且つ、ユーザのセキュリティレベルにかかわりなく、ネットワーク配信は、ログを記録することと、プリント制限をかけること、信頼できるチャネルを使用することの要件を満たすときに許可されることを示している。

【００６６】

そして、ルール３は、図２の第２４行目の<acc_rule>から、第３０行目の<user_security_level>ANY</user_security_level>までの部分及び、第３１行目<operation>から、第３５行目</operation>までの部分により記述される。

【００６７】

第２５行目の<doc_category>ANY</doc_category>は、文書カテゴリーにかかわりないことを示す。

【００６８】

第２６行目の<doc_security_level>high</doc_security_level>は、
文書のセキュリティレベルがhighの場合を示す。

【００６９】

第２９行目の<user_category>DOC-CATEGORY</user_category>は、ユーザのカテゴリーが文書のカテゴリーと同じであることを示す。

【００７０】

第３０行目の<user_security_level>ANY</user_security_level>は、ユーザの

セキュリティレベルにかかわりないことを示す。

【００７１】

第３２行目から第３４行目の、

<name>scan</name>

<requirement>audit</requirement>

<requirement>embed_trace_info</requirement>

は、読み取りは、「ログを記録すること」及び、「追跡可能な情報を埋め込むこと」の要件を満たすときに許可される。

【００７２】

従って、ルール３では、第２５行目、第２６行目、第２９行目、第３０行目、第３１行目から第３４行目により、文書カテゴリーにかかわりなく、文書のセキュリティレベルが”high”の場合には、ユーザのカテゴリーが文書のカテゴリーと同じであり、且つ、ユーザのセキュリティレベルにかかわりなく、読み取りは、ログを記録することと、追跡可能な情報を埋め込むことの要件を満たすときに許可されることを示している。

【００７３】

ここで、「追跡可能な情報を埋め込むこと」には、例えば、電子すかしの埋め込み、表示可能なラベルの埋め込み、文書属性情報の追加などを含んでも良い。また、表示可能なラベルは、読み取りを指示したユーザの認証データと読み取りを指示した時点のタイムスタンプを含んでもよい。さらに、「ログを記録すること」には、読み取りを指示したユーザの認証データと、読み取り対象の文書データと、読み取りを指示した時点のタイムスタンプをログに記録するようにしてもよい。また、「ログを記録すること」には、ネットワーク配信を指示したユーザの認証データとネットワーク配信先の情報と、読み取り対象の文書データと、読み取りを指示した時点のタイムスタンプをログに記録するようにしてもよい。

【００７４】

次に、図２に示したセキュリティポリシーを使用して、図１に示した本発明の実施例の文書読み取り装置が文書を読み取り又は、読み取った文書をネットワークに配信する場合の実施例について説明する、

先ず最初に、文書読み取り装置が文書を読み取る場合の実施例について説明する。

【００７５】

先ず最初に、ステップＡ１で、ユーザが、読み取り装置１００に紙文書を設置し、オペレーションパネル１０１から、紙文書の読み取り指示１１０を入力する。

【００７６】

次に、ステップＡ２で、読み取り手段１０６が、紙文書の読み取りを行う。

【００７７】

次に、ステップＡ３で、文書属性取得手段１０４は、読み取った文書データのバーコードや電子透かしなどの画像情報から、文書ＩＤを抽出し、データベース１０２に登録されている文書ＩＤに対応するカテゴリー、セキュリティレベルを取得し、読み取り手段１０６に通知する。

【００７８】

次に、ステップＡ４で、読み取り手段１０６は、上記の文書属性取得手段１０４が通知した文書属性に従って、セキュリティポリシー１０５の中の対応するエントリを検索して、要件を抽出する。

【００７９】

上述の図２に示すセキュリティポリシーに基づいて、例えば、セキュリティレベルが”basic”の文書を読み取りしようとしている場合には、抽出すべき要件はない。

【００８０】

また、上述の図２に示すセキュリティポリシーに基づいて、例えば、セキュリティレベルが”high”の文書を読み取りしようとしている場合には、前述のように、「ログを記録すること」及び「追跡可能な情報を埋め込むこと」が、読み取りの要件となる。「ログを記録すること」及び「追跡可能な情報を埋め込むこと」の内容に関しては、上述と同様である。

【００８１】

次に、ステップＡ５－１で、上述のステップ４のセキュリティレベルが”basi

c”のときの場合のように、抽出すべき要件がない場合には、読み取り手段は文書の読み取りを行って、ユーザは文書データを取得して終了する。

【００８２】

一方、ステップＡ５－２では、上述のステップ４のキュリティレベルが”high”のときの場合のように、抽出すべき要件がある場合には、読み取り手段はその要件をすべて満たすことができるかを判定する。

【００８３】

ステップＡ５－２の場合には、次に以下のステップ６－１と６－２が実行される。

【００８４】

ステップＡ６－１では、すべての要件を満たすことができない場合は、ユーザに通知をして、読み取りデータを破棄して終了する。

【００８５】

次に、ステップＡ６－２では、すべての要件を満たすことができる場合は、その要件を満たした読み取りを行って、ユーザは文書データを取得して終了する。この場合には、ステップＡ６－２では、以下のステップ、Ａ７－１からＡ７－６が実行される。

【００８６】

ステップＡ７－１では、ユーザ属性取得手段１０３は、オペレーションパネル１０１から読み取り指示１１０を出したユーザに、ユーザＩＤの入力要求を出す。

【００８７】

次に、ステップＡ７－２では、ユーザは、オペレーションパネル１０１からユーザＩＤを入力する。

【００８８】

次に、ステップＡ７－３では、ユーザ属性取得手段１０３は、ユーザＩＤからデータベース１０２に登録されている入力されたユーザＩＤに対応するカテゴリー、セキュリティレベルを取得し、読み取り手段１０６に通知する。

【００８９】

次に、ステップＡ７－４では、ログを記録する。

【００９０】

そして、ステップＡ７－５では、読み取った文書データに追跡可能な情報の埋め込み(例えば、電子すかしの埋め込み、表示可能なラベルの埋め込み、文書属性情報の追加など)を行う。表示可能なラベルは、読み取りを指示したユーザの認証データと読み取りを指示した時点のタイムスタンプを含んでもよい。

【００９１】

最後に、ステップＡ７－６で、ユーザは文書データを、読み取りデータ１０７内に取得して終了する。

【００９２】

以上のように、図２に示したセキュリティポリシーを使用して、図１に示した本発明の実施例の文書読み取り装置が文書を読み取ることができる。

【００９３】

次に、文書読み取り装置が文書を読み取り且つ読み取った文書をネットワークに配信する場合の実施例について説明する。

【００９４】

先ず最初に、ステップＢ１で、ユーザが、読み取り装置１０６に紙文書をセットし、オペレーションパネル１０６から、読み取りデータの配信先の指定及び紙文書の読み取り指示１１０を出す。

【００９５】

次に、ステップＢ２で、読み取り手段１０６が、紙文書の読み取りを行う。

【００９６】

次に、ステップＢ３で、文書属性取得手段１０４は、読み取った文書データのバーコードや電子透かしなどの画像情報から文書ＩＤを抽出し、データベース１０２に登録されている文書ＩＤに対応するカテゴリー、セキュリティレベルを取得し、読み取り手段１０６に通知する。

【００９７】

次に、ステップＢ４では、読み取り手段１０６は、上記の文書属性取得手段１０４が通知した文書属性に従って、セキュリティポリシー１０５の中の対応する

エントリを検索し、要件を抽出する。

【００９８】

上述の図２に示すセキュリティポリシーに基づいて、例えば、セキュリティレベルが”basic”の文書を読み取り、ネットワーク配信しようとしている場合には、読み取りに関する要件はない。しかし、上述のように、ネットワークに配信する時には、「ログを記録すること」と「プリント制限をかけること」と「信頼できるチャネルを使用すること」が要件となる。

【００９９】

また、上述の図２に示すセキュリティポリシーに基づいて、例えば、セキュリティレベルが”high”の文書を読み取りしようとしている場合には、読み取りに関する要件として、「ログを記録すること」と「追跡可能な情報を埋め込むこと(例えば、上述のような、電子すかしの埋め込み、表示可能なラベルの埋め込み、文書属性情報の追加など)」が要件となる。しかし、ネットワークに配信することを許可するルールがないため、許可されない。

【０１００】

次に、例えば、文書をネットワークへ配信する際の要件が、セキュリティーポリシー１０５内に存在しない場合には、ステップＢ５－１では、読み取り手段１０６は文書をネットワークポート１０８を介してネットワークへ配信して、処理を終了する。

【０１０１】

一方、例えば、文書をネットワークへ配信する際の要件が、セキュリティーポリシー１０５内に存在する場合には、ステップ５－２で、読み取り手段１０６が、その要件をすべて満たすことができるかを判定する。

【０１０２】

ステップＢ５－２の場合には次に、ステップＢ５－３で、ネットワークに配信することを許可するルールがない場合には、読み取り手段１０６が、ユーザに、「ネットワークに配信することを許可するルールがない」ことを通知をして、読み取りデータを破棄して終了する。例えば、これは、上述のステップＢ４の、セキュリティレベルが”high”の場合である。

【０１０３】

次に、ステップＢ６－１では、すべての要件を満たすことができない場合は、ユーザに通知をして、読み取りデータを破棄して終了する。

【０１０４】

次に、ステップＢ６－２では、例えば、上述のセキュリティレベルが”basic”の場合のように、すべての要件を満たすことができる場合は、その要件を満たした読み取り及び、文書をネットワークに配信して終了する。この場合には、ステップＢ６－２では、以下のステップ、Ｂ７－１からＢ７－６が実行される。

【０１０５】

ステップＢ７－１では、ユーザ属性取得手段１０６は、オペレーションパネル１０１から、読み取り指示１１０を出したユーザに、ユーザＩＤの入力要求を出す。

【０１０６】

次に、ステップＢ７－２では、ユーザは、オペレーションパネル１０１からユーザＩＤを入力する。

【０１０７】

次に、ステップＢ７－３では、ユーザ属性取得手段１０３は、ユーザＩＤからデータベース１０２に登録されている入力されたユーザＩＤに対応するカテゴリー、セキュリティレベルを取得し、読み取り手段１０６に通知する。

【０１０８】

次に、ステップＢ７－４では、ログを記録する。

【０１０９】

そして、ステップＢ７－５では、読み取った文書データを、印刷不可能なデータ(たとえばADOBE（登録商標）の印刷禁止属性を持ったPDFなど)に変換する。

【０１１０】

最後にステップＢ７－６では、信頼できる通信経路(たとえばIPsecやVPNなど)を通じて、文書を、ネットワークポート１０８を介してネットワークへ配信し、終了する。

【０１１１】

以上のように、図２に示したセキュリティポリシーを使用して、図１に示した本発明の実施例の文書読み取り装置が、文書を読み取り且つ読み取った文書をネットワークに配信することができる。

【０１１２】

【発明の効果】

以上説明したように、本発明によって、セキュリティポリシーに基づいた文書の読み取り装置、読み取り方法、ネットワーク配信を行う装置及びネットワーク配信を行う方法、その方法を実行するプログラム、そのプログラムを記憶した記憶媒体、及び伝送装置を提供することができる。

【図面の簡単な説明】

【図１】

本発明の実施例の文書読み取り装置の構成を示す図である。

【図２】

ＸＭＬ（Ｅｘｔｅｎｓｉｂｌｅ　Ｍａｒｋｕｐ　Ｌａｎｇｕａｇｅ）により記述した、本発明の実施例のセキュリティポリシーを示す図である。

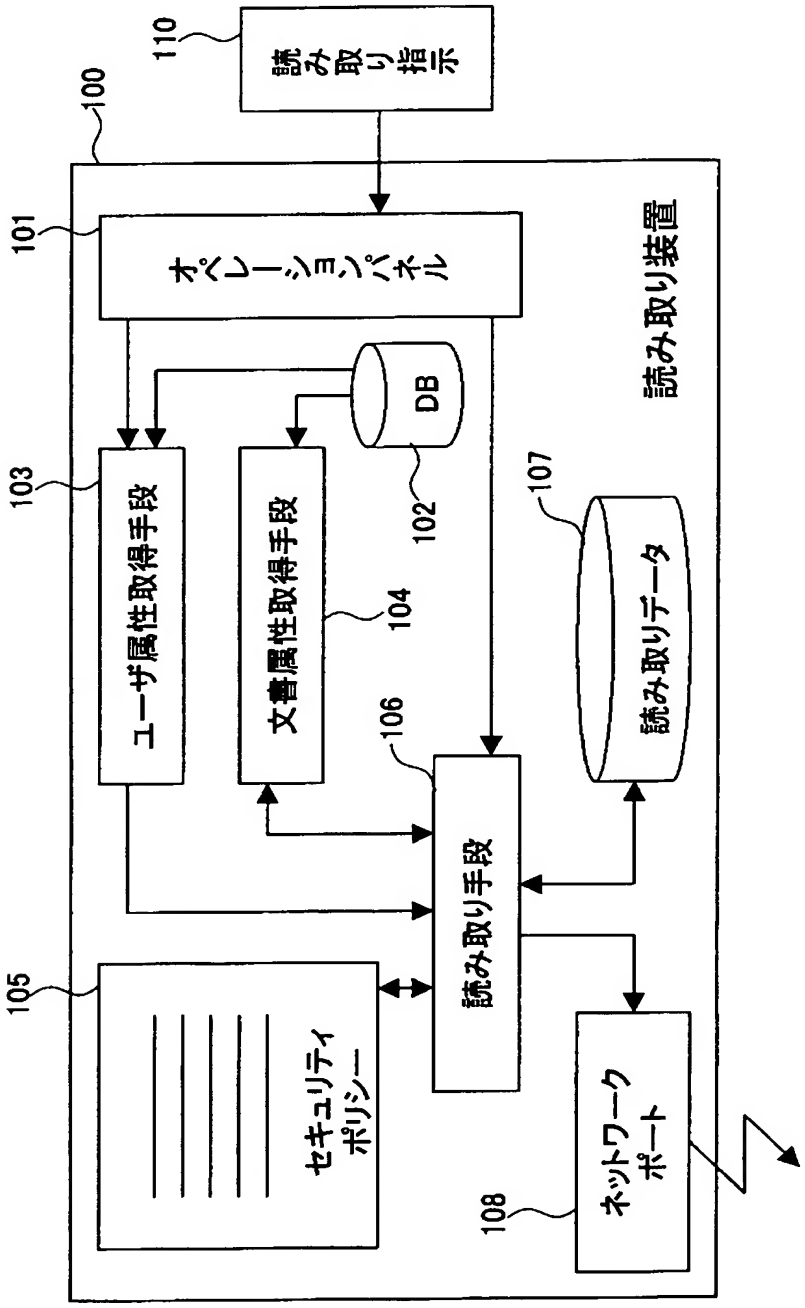
【符号の説明】

１００　文書読み取り装置
１０１　オペレーションパネル
１０２　データベース
１０３　ユーザ属性取得手段
１０４　文書属性取得手段
１０５　セキュリティーポリシー
１０６　読み取り手段
１０７　読み取りデータ
１０８　ネットワークポート
１１０　読み取り指示

【書類名】　図面

【図１】

本発明の実施例の文書読み取り装置の構成を示す図



【図２】

XML(Extensible Markup Language)により記述した本発明の実施例のセキュリティポリシーを示す図

```
<?xml version="1.0" encoding="SHIFT-JIS" ?>
<document_security_policy>
<policy>
  <acc_rule>
    <doc_category>ANY</doc_category>
    <doc_security_level>basic</doc_security_level>
    <acl>
      <ace>
        <user_category>ANY</user_category>
        <user_security_level>ANY</user_security_level>
        <operation>
          <name>scan</name>
          <allowed/><!-- allowed without any requirement -->
        </operation>
        <operation>
          <name>net_delivery</name>
          <requirement>audit</requirement>
          <requirement>print_restriction</requirement>
          <requirement>trusted_channel</requirement>
        </operation>
      </ace>
    </acl>
  </acc_rule>
  <acc_rule>
    <doc_category>ANY</doc_category>
    <doc_security_level>high</doc_security_level>
    <acl>
      <ace>
        <user_category>DOC-CATEGORY</user_category>
        <user_security_level>ANY</user_security_level>
        <operation>
          <name>scan</name>
          <requirement>audit</requirement>
          <requirement>embed_trace_info</requirement>
        </operation>
      </ace>
    </acl>
  </acc_rule>
</policy>
```

【書類名】　　要約書

【要約】

【課題】　文書に関するセキュリティポリシーに基づいて、紙文書の読み取り、ネットワークへの配信を行う方法を提供する。

【解決手段】　ユーザ属性を取得し、文書属性を取得し、ユーザ属性と文書属性との組み合わせに対して読み取りが許可されているかをセキュリティポリシーにより判断し、許可されていない場合にはデータを破棄して終了し、許可されている場合には対応する要件をセキュリティポリシーから抽出し、要件がセキュリティポリシー内に存在しない場合には文書の読み取りを行って終了し、要件がセキュリティポリシー内に存在する場合にはすべての要件を読み取る方法で実行可能であるかを判定し、実行可能でない要件が存在する場合にはデータを破棄して終了し、すべての要件を実行可能である場合には抽出された前記要件を満たして文書の読み取りを行って終了する、セキュリティポリシーに基づいて文書を読み取る方法により実現する。

【選択図】　　図１

特願２００２－２７５９７３

出　願　人　履　歴　情　報

識別番号　　［０００００６７４７］

１．変更年月日　　１９９０年　８月２４日
［変更理由］　　新規登録
住　所　　東京都大田区中馬込１丁目３番６号
氏　名　　株式会社リコー

２．変更年月日　　２００２年　５月１７日
［変更理由］　　住所変更
住　所　　東京都大田区中馬込１丁目３番６号
氏　名　　株式会社リコー